

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Morris et al.

SERIAL NO.: 10/727,291

GROUP: 2137

FILED: 12/3/2003

EXAMINER: Williams

---

Declaration – Rule 1.132 pursuant to 37 CFR 41.33

I, Thomas P. Yohe, hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I am the inventor in the above-identified application. I hereby state as follows:

1. This is a Declaration in response to the Office Action of 1/22/2008 wherein the Examiner stated applicant's original disclosure does not provide support for the amendments made in response to the final office action dated 10/1/2007, particularly, the disclosure did not provide for first and second SSL connection...
2. The original disclosure in applicants' application at page 6, lines 2-22, page 7, lines 1-22 and page 8, lines 1-2 of the filed Specification, the following is stated with the bracketed text **[i.e., a first SSL connection]** and **[i.e., a first SSL connection]** indicating

added language for the examiner's understanding of the first and second SSL connections. It will be understood by such language to those skilled in the art that the portions of text preceding and proximate the bracketed text does equate to first and second SSL connections: The page 6, lines 2-22, page 7, lines 1-22 and page 8, lines 1-2 of the filed Specification is:

The present invention is generally depicted in FIGS. 2A and 2B and is directed to a system and method for increasing data access in a secure socket layer network environment and is generally designated by the number 100. The system 100 includes a *web server computer 102* which has an operating system/software, server software, memory and linking devices as is known in the art. Further, the *computer 102 has SSL protocol server software operably disposed thereon for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key.*

A *client computer 104* includes an operating system/software, web browser software having SSL protocol client software operably disposed *thereon for enabling a SSL connection*, memory and linking devices as is known in the art and is communicatively linked to the web server computer 102. SSL acceleration client (SSLAC) software is operably disposed on the client computer 104 for monitoring when the web browser requests a SSL connection with the web server 102.

*SSL acceleration server (SSLAS) software is operably disposed on the web server computer 104 for receiving a request for a SSL connection through SSL acceleration client software.* The SSL acceleration server software is operably associated with the SSL protocol server software to obtain one either a copy or an equal credential of the CA certificate (i.e., a pseudo CA certificate) and private key.

The operation of the invention can be understood from steps shown in FIGS. 2A and 2B. *SSL acceleration client software intercepts 200 new SSL request for a SSL secure connection from the web browser to a target web server. The SSL acceleration client software then initiates 202 a SSL handshake with the SSLAS operably associated with the target web server computer and to start SSL connection.* The SSLAS then determines 204 which CA certificate is operably associated with the target web server. As part of the SSL handshake between SSLAC and SSLAS, the SSLAS sends 206 this CA certificate to SSLAC along with a public key. *At this point a secure SSL session is established between SSLAC and SSLAS and all subsequent data traffic between SSLAC and SSLAS flows over this secure connection. [i.e., a first SSL connection]* The SSLAC software sends 208 the copy of the CA certificate to the web browser for validation 210. Web browser software sends 212 a list of available encryption algorithms (ciphers) back to target web server (i.e., server computer 102). SSLAC software intercepts this from the browser and sends 214 a chosen cipher to the

*browser software. The web browser software creates 216 a secret key, encrypts using chosen cipher and using the previously received public key and sends 218 the encrypted secret key to the target server, which is intercepted and sent 219 through the SSL acceleration client software to the SSLAS software. SSLAS software de-encrypts 220 the secret key using the private key operably associated with the target server. SSLAS software sends 222 decrypted secret key back to SSLAS software via the secure SSL connection, wherein a “handshake” is completed and secure communications between the client computer’s web browser and SSLAS software e [i.e., a second SSL connection] and by using the secret key, data can be accelerated between the client computer 104 and the web server computer 102 employing acceleration software, such as compression software of the SSL acceleration client/server software.*

Because the SSL connection is terminated by SSLAC, *SSLAC can process the data in unencrypted form allowing it to apply data compression and other optimization techniques to the data stream.* This is done in such a way that the credentials of the SSLAS are presented to the web browser without having violated the SSL paradigm because the private key of the SSLAS was never transmitted to SSLAC.

3. The specification clearly discloses a client computer, web server, first and second SSL connections wherein the second permits optimization techniques to be applied on the data transmitted through the second SSL connection. Accordingly, withdrawal of the rejection to the specification and drawings is kindly requested.

4. The thrust of the examiner’s position is that the claimed invention is obvious in view of Aziz teaching multiple connections as seen in FIG. 3 (330). However, Aziz fails to show multiple SSL connections between the same client and server. Rather, Aziz simply shows the inclusion of the means to create a single secure connection between each client/relay and relay/server using conventional SSL connection technology.

It is clear that Aziz only discloses making a single connection between each client and a relay and a relay and a server.

5. Gast is directed to a system and method for accelerating cryptographically

secured transactions. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce latency [paragraph 0015]. Gast simply moves the task of processing the security mechanism, i.e., establishing a SSL session to a central control point [0022]. The point stressed in Gast is to offload the establishment of SSL connections by the server, not to establish additional SSL connection between the client and server as opposed to the instant invention which provides a CA certificate and a pseudo CA certificate to establish concurrent SSL connections through whereby data can pass in a compressed form, for example, in the second established connection. Gast teaches away from the instant invention.

6. Freed et al. discloses a secure sockets layer architecture which employs an intermediate device between the client computer and the server computer which intercepts SSL/TCP data and then performs one or more transactions to aid in acceleration. Like Aziz, there is no direct link between the client computer and the server computer. As seen in paragraphs [0007-0010] of Freed et al., there is merely a conventional SSL handshake which is employed and all secure data is sent through the one secure tunnel which is created. Freed et al are concerned with offloading the server the task of encryption/decryption task by employing a tertiary or intermediary device to interact with the client and the server. Nevertheless, the tertiary computer employs conventional handshake technology.

7. The Examiner failed to correctly appreciate and consider all of the limitations in the claimed invention as properly interpreted in the applicants' specification.

The instant invention provides a server with SSL protocol server software and SSL acceleration server software on both the client and server for enabling direct and multiple SSL sessions to take place through the use of creating a pseudo CA certificate on the web server in addition to having the existing CA certificate on the web server which are presented to the client computer having SSL protocol and SSL acceleration software thereon. By so providing, multiple direct secure links are created between the same two computers. None of the cited art provides this combination of elements.

The instant invention enables secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, such as when connecting to a secure bank site, for example. In addition, the instant invention provides the pseudo CA certificate and secondary SSL connection through which data may pass in a secure connection which enables functional operations (optimization techniques) to be performed thereon, such as compression of data. This is not taught, disclosed or suggested in Freed et al. (Gast or Aziz) and this can't be accomplished in the teachings of Freed et al. or Aziz (or Gast). Freed et al. only acts as an intermediary intercepting all communication over the existing SSL connection and passes the data accordingly, paragraph [0039]. Paragraphs [0052] - [0053] and the claims in Freed et al. further illustrate Freed et al. are only concerned with providing a classic SSL connection between the client and server through an intermediary device.

8. The issue before us is therefore whether the combination Aziz alone or in combination with Gast or freed et al. renders claims 1 through 19 unpatenable under 35 USC § 103 (a)? Particularly, does the proffered combination teach a method or system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key; and

a client computer communicatively linked to the web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second SSL connection? The answer to this question must be in the negative.

As set forth above, none of the art discloses the claimed elements alone or in combination. Thus, the first step of the 103 analysis is not met. One of ordinary skill in the art would have readily recognized that the Aziz, Gast, Freed et al. combination, at best, teaches a system for allowing a client computer and server computer to employ conventional SSL technology to provide single SSL connections therebetween to transmit secure data.

9. However, the ordinarily skilled artisan would have also recognized that the cited combination does not lend itself to the system of the instant invention whereby a single

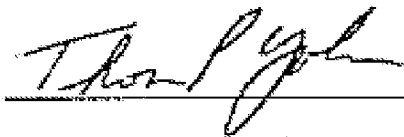
client computer server relation is equipped to establish two SSL connections to transfer secure data over the second connection in a manner which enables functional operations (optimization techniques) to be performed thereon. In other words, the proffered combination teaches a system which is limited and not capable of such operations. It is silent as to a system (or how to make a system as claimed in the instant invention) enabling such multiple SSL connections between the same server and client computer. It follows that applicants have shown that the instant invention is patentable.

10. It is respectfully submitted that the instant claimed invention is not taught, disclosed or suggested by Aziz, Gast or Freed et al. taken alone or together. The instant invention is respectfully submitted to be patentably distinct over the art of record.

Withdrawal of the rejection of claims 1-19 is respectfully requested.

Further, the declarant sayeth not.

Full name of inventor: Thomas P. Yohe



---

Inventor's signature

Date 2/1/2008